# Introduction to Cyber Security

## Data Centre Security, Cloud Computing and Data Security

March 2021

# Agenda

In today's session, you will learn about:

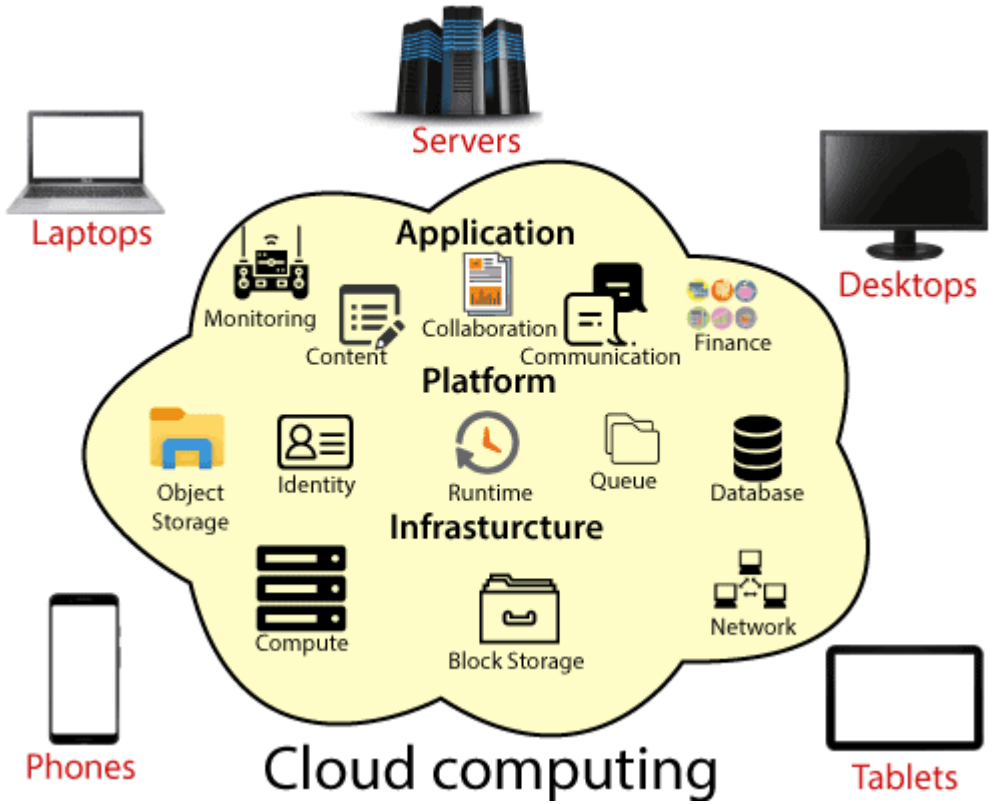
- Data Centre Security
- Cloud Computing
- Data Security

Source: Freepik

# What is Cloud Computing?

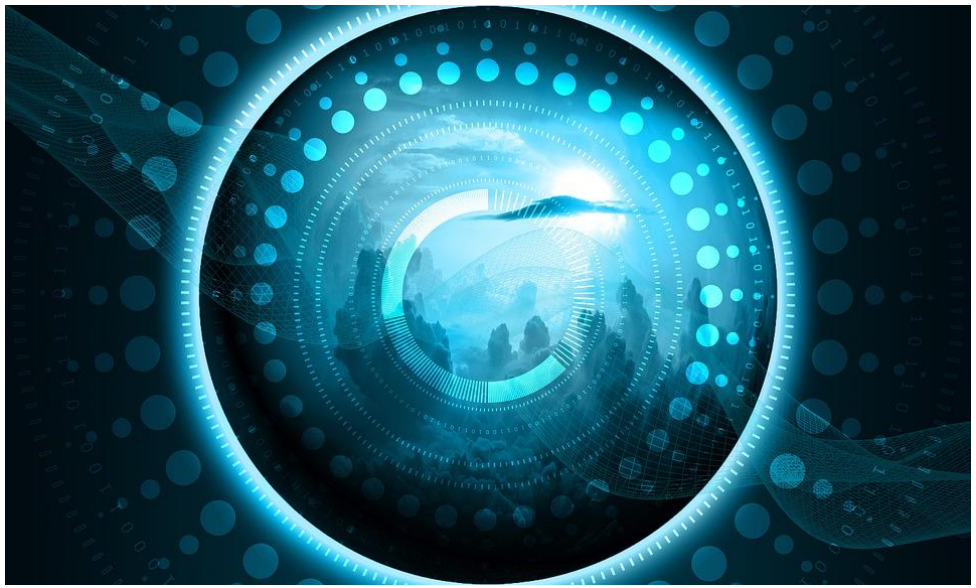
Created by fae frey
from Noun Project

Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, intelligence, and more, over the Cloud (Internet).



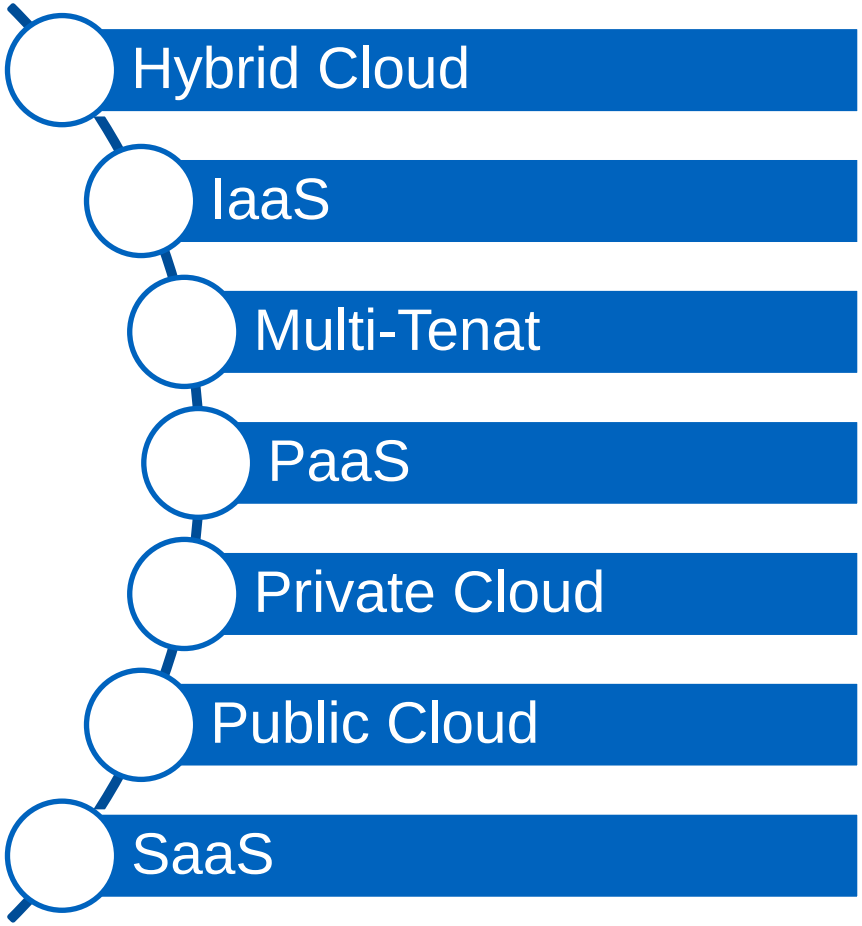
Advantages of cloud computing

- Cost
- Speed
- Scalability
- Productivity
- Reliability
- Security



Source: Pixabay

# Types of Cloud Computing and Services



## Name of the Activity

**Face off**

## Instructions

Mode: **In-session**

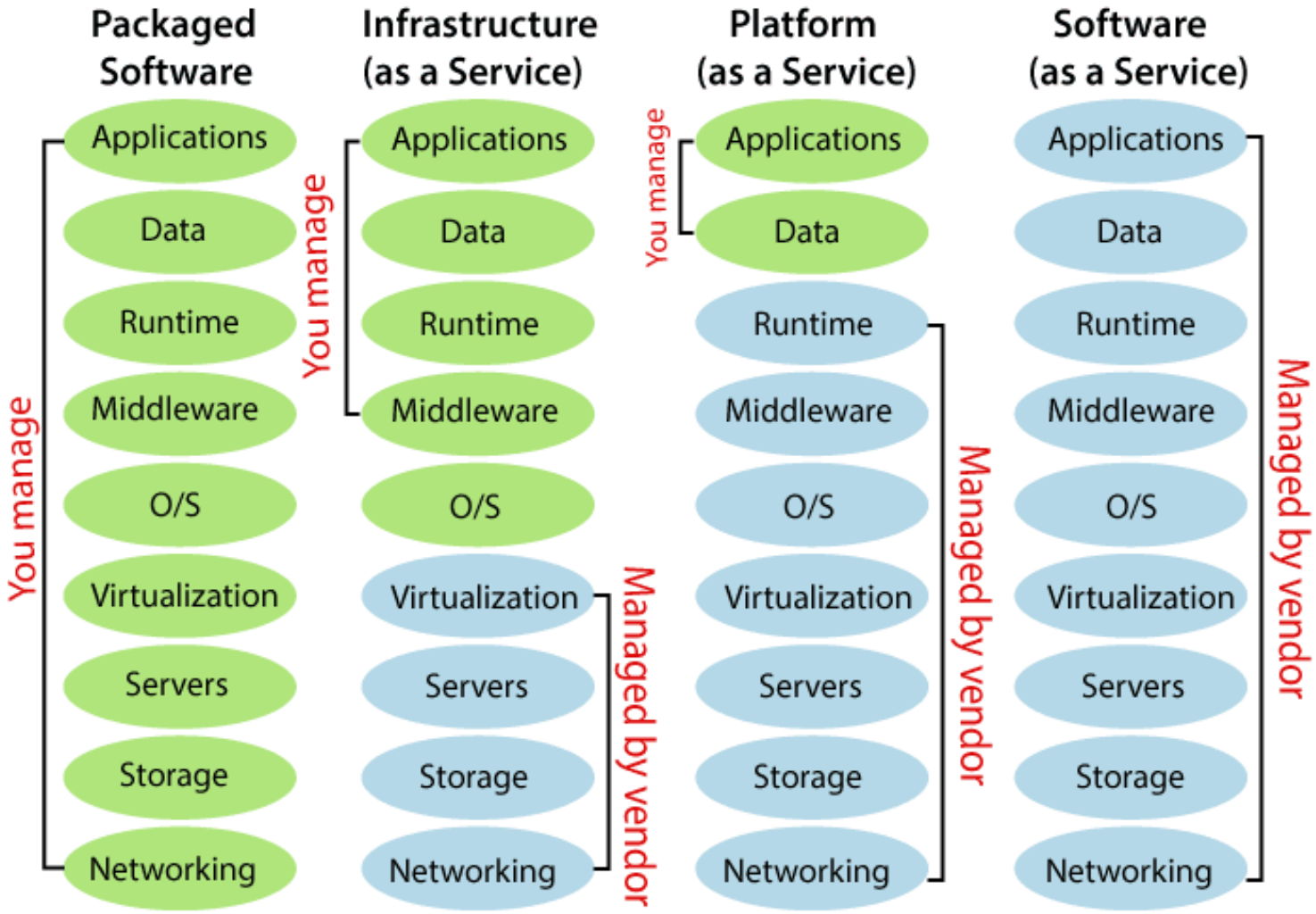
Duration: **5 minutes**

Materials Required: **None**

# Activity – Face Off

Difference between
Iaas and Saas

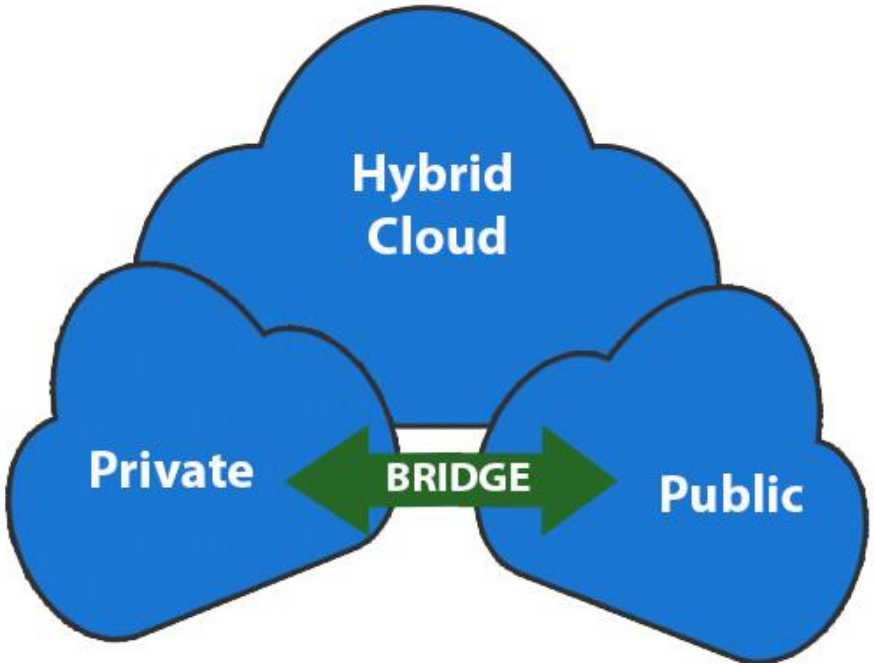
# Types of Cloud Services

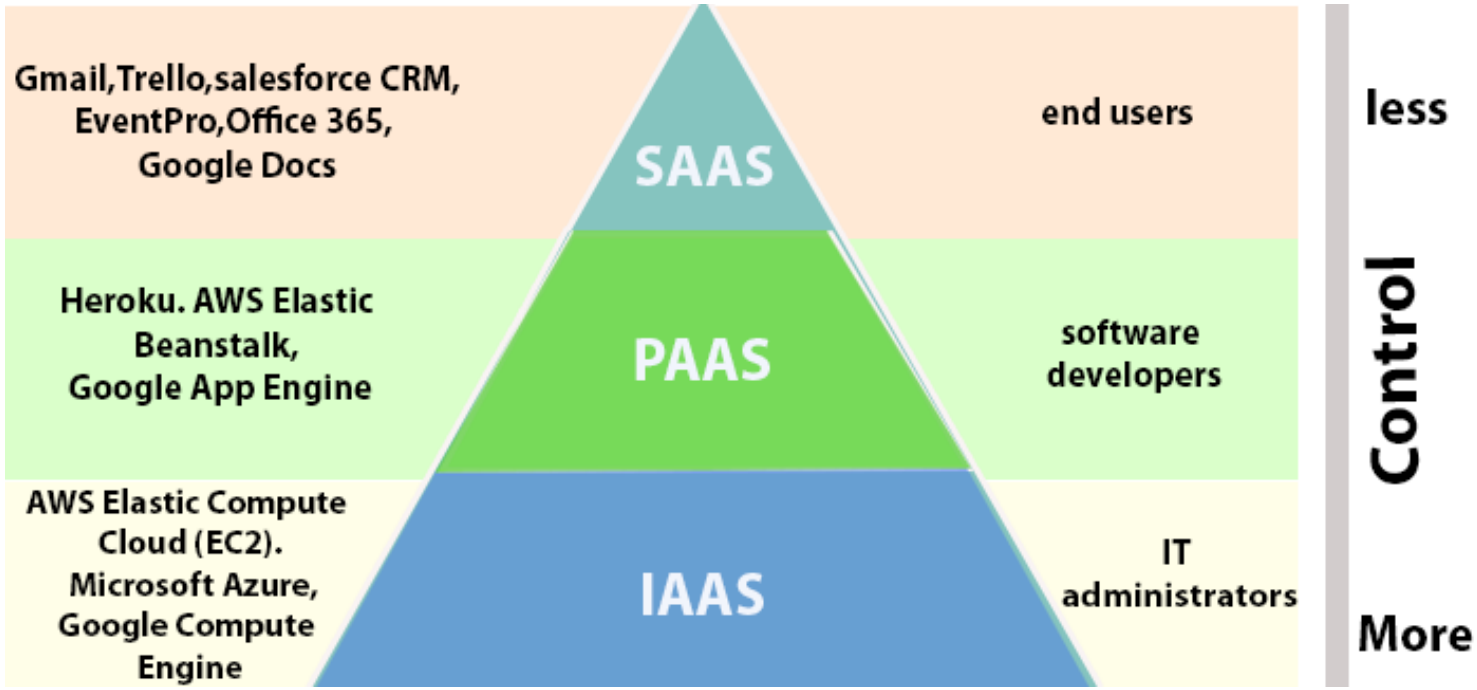


# What are the different types of Cloud Services?

Created by fae frey
from Noun Project

# Types of Cloud Services



# Benefits of Cloud Computing

Benefits:

- Mobility
- Easy to scale server resources
- Safety from server hardware issues and loss prevention
- Faster website speed and performance
- Automatic software updates
- Sustainability

Source: The Noun Project

# What is Encryption?

Created by fae frey
from Noun Project

# Key Technologies for Cloud Security

A cloud security strategy should include all of the following technologies:

- Encryption
- Identity and Access Management (IAM)
- Firewall

Source: The Noun Project

# Practices for keeping cloud data secure

A cloud security strategy should include all of the following technologies:

- Proper configuration of security settings for cloud servers
- Consistent security policies across all clouds and data centers
- Backup Plans
- User and employee education:

Source: The Noun Project

## Name of the Activity

**Behind the Door Number**

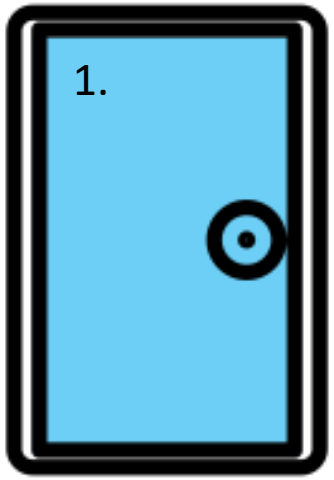
## Instructions

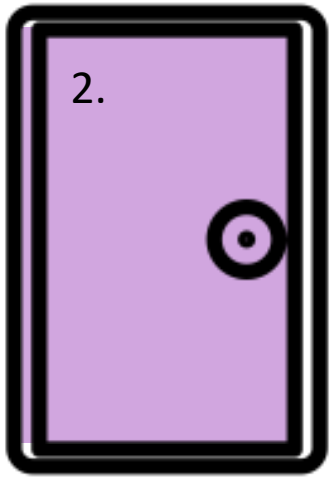
Mode: **In-session**

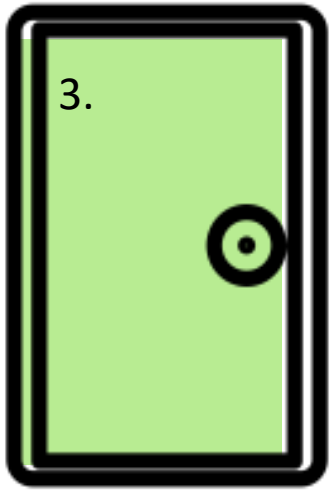
Duration: **5 minutes**

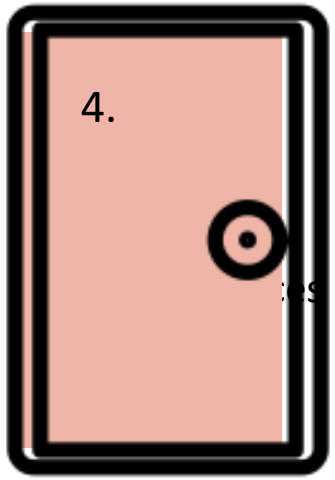
Materials Required: **None**

# Knowledge Check – Behind the Door Number




Source: Noun project

# Data Center

- A data center houses servers and/or data storage for an organization.
- A data center can be a single server or complex with hundreds of servers on racks.

Source: Freepik

# Cloud Companies

- Cloud companies have their own data centers, organizations often have their own data centers as well, which are referred to as on-premises.
- When most people talk about their data centers, the implication is that they are talking about on-premises data centers.

Source: Freepik

# What is a Data Breach?

Created by fae frey
from Noun Project

# Threats and Attacks

- Data breaches
- Insufficient identity, credential and access management
- Insecure interfaces and APIs
- System vulnerability
- Account or service hijacking

Source: The Noun Project

# What is a Malicious Insider?

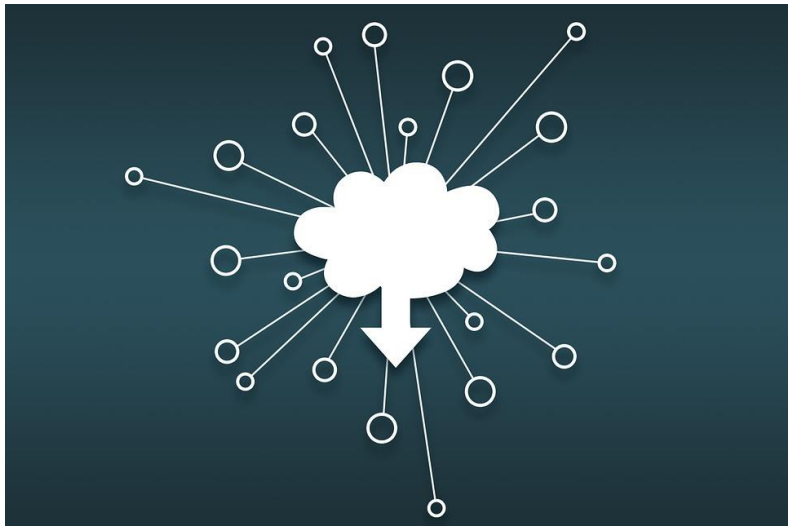
Created by fae frey
from Noun Project

- Malicious insider
- Data loss
- Lack of due diligence
- Abuse and nefarious use of cloud services
- Shared technology vulnerabilities

Source: The Noun Project

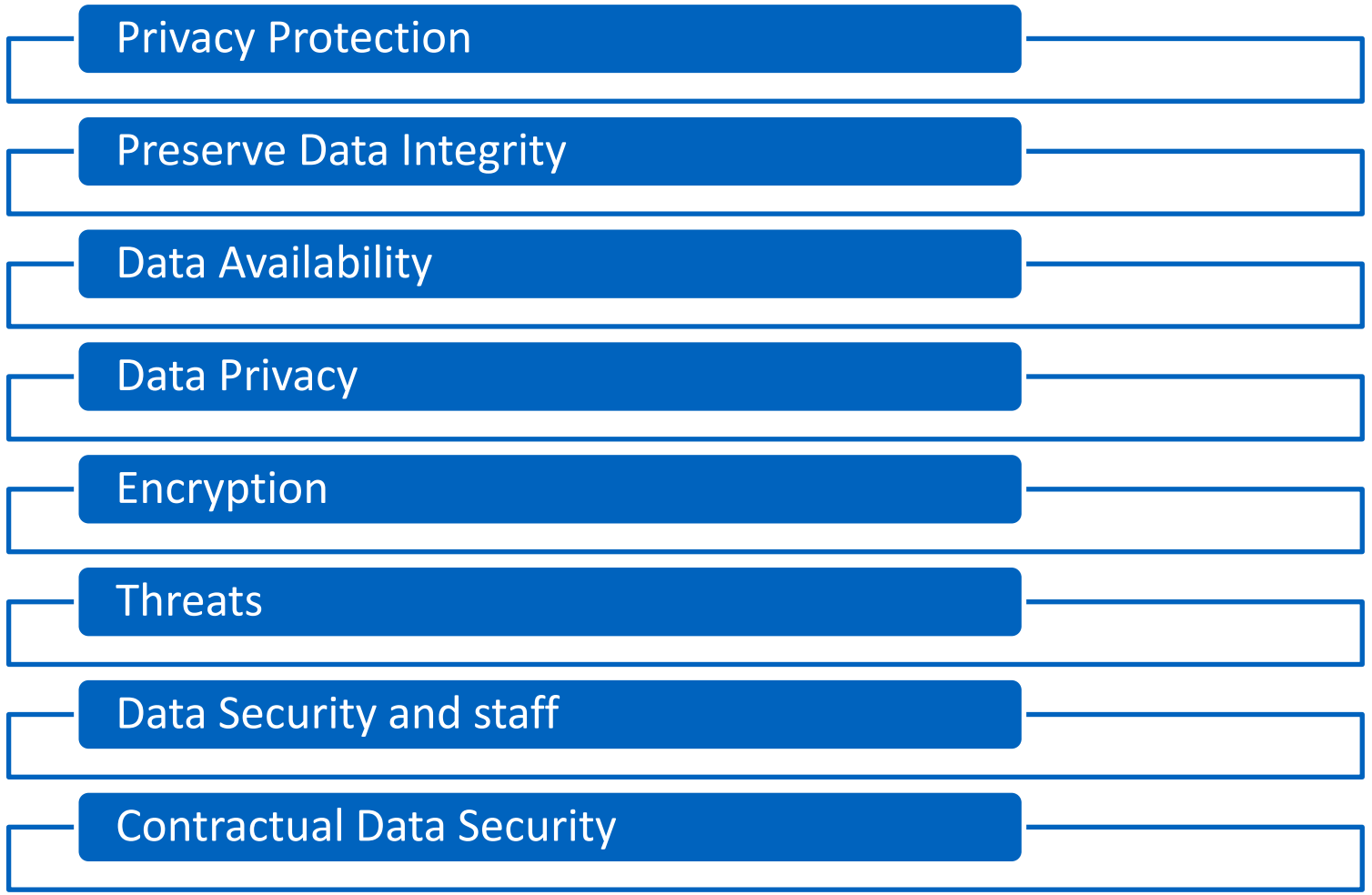
# Security in Cloud

- Protection against DDoS
- Data security
- Regulatory compliance
- Flexibility
- High availability and support



Source: Pixabay

These are the eight critical concepts for data security in the cloud:



# Privacy Protection

- Identify the sensitive data types and define them.
- There are automated tools to help discover and identify an organization’s sensitive data and where it resides.

# Preserve Data Integrity

- Data integrity can be defined as protecting data from unauthorized modification or deletion.
- In a cloud, especially a multi-cloud environment, could get tricky. Since there are a large number of data sources and means to access, authorization becomes crucial in assuring that only authorized entities can interact with data.

# Data Availability

- Downtime is a fact of life and all you can do is minimize the impact. This is where the service-level agreement (SLA) is vital and paying a close eye to details really matters.
- Every cloud storage service has a particular strength: Amazon's Glacier is ideal for mass cold storage of rarely accessed data, Microsoft's Azure blob storage is ideal for most unstructured data, while Google Cloud's SQL is tuned for MySQL databases.

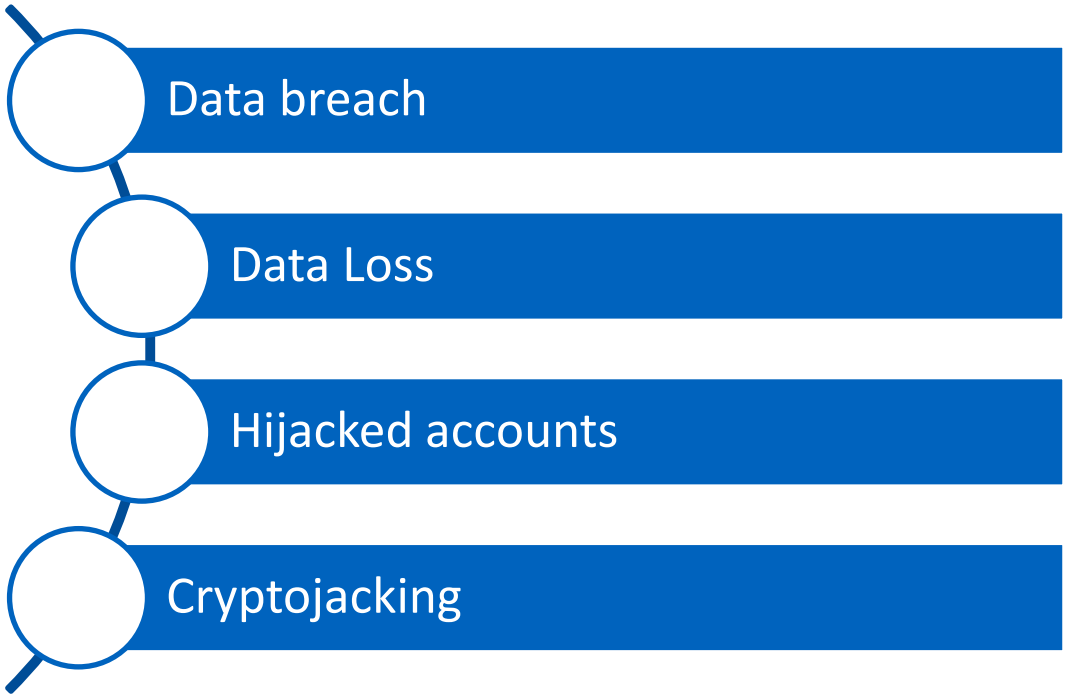
# Data Privacy

- Privacy laws have forced more than a few companies to say no to the cloud because they can’t make heads or tails of the law or it’s too burdensome. And it’s not hard to see why.
- Many providers may store data on servers not physically located in a region as the data owner and the laws may be different.

# Encryption

- Encryption is the means for which data privacy is protected and insured, and encryption technologies are fairly mature.
- Virtually every cloud storage provider encrypts the data while it is in transfer.
- Many cloud services offer key management solutions that allow you to control access because the encryption keys are in your hands.

- Cloud service providers have a variety of security tools and policies in place but problems still happen, usually originating in human error.



# Data Security and Staff

- Most employee-related incidents are not malicious.
- According to the Ponemon Institute's *2016 Cost of Insider Threats Study*, 598 of the 874 insider related incidents in 2016 were caused by careless employees or contractors.
- However, it also found 85 incidents due to imposters stealing credentials and 191 were by malicious employees and criminals.

# Contractual Data Security

- The SLA should include a description of the services to be provided and their expected levels of service and reliability.
- There are multiple checkmarks for a SLA.
  - Specifics of services provided, such as uptime and response to failure.
  - Definitions of measurement standards and methods, reporting processes, and a resolution process.
  - An indemnification clause protecting the customer from third-party litigation resulting from a service level breach.

## Name of the Activity

**Behind the Door Number**

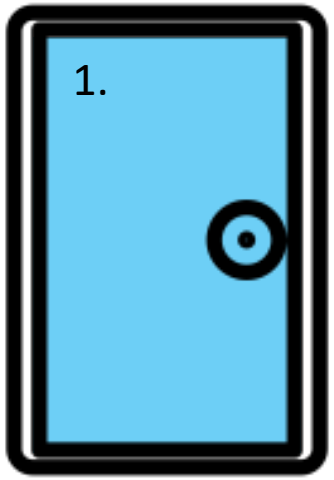
## Instructions

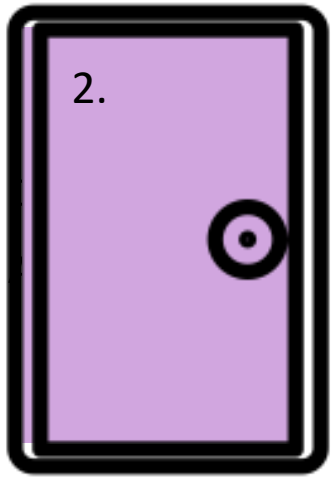
Mode: **In-session**

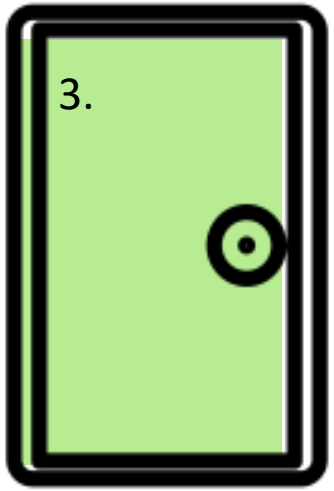
Duration: **5 minutes**

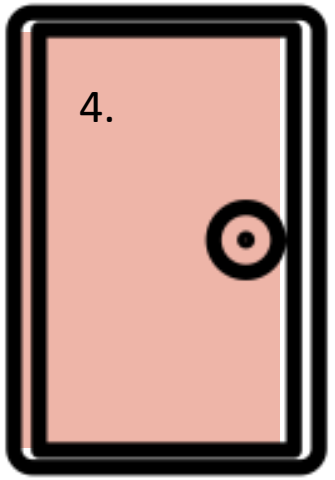
Materials Required: **None**

# Knowledge Check – Behind the Door Number




Source: Noun project

## Name of the Activity

**Fill in the Blanks**

## Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

# Activity – Fill in the Blanks

1. When top cloud computing security solutions help companies in regulated industries by managing and maintaining enhanced infrastructures it is called _____ .

   **Regulatory Compliance**

2. _____ occurs in cloud due to interaction with risks within the cloud or architectural characteristics of the cloud application.

   **Data Loss Threat**

3. _____ is when multiple users access the same public cloud.

   **Multi Tenant**

4. _____ is combination of both the private and public cloud. .

   **Hybrid Cloud**

5. An _____ may access and re-use these APIs or passwords. .

   **Unauthorized User**

# Summary

In this session, you learnt about:

- Data Centre Security
- Cloud Computing
- Data Security